§170.315(d)(3) Audit report(s)

2015 Edition Cures Update CCG

Version 1.0 Updated on 06-15-2020

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	06-15-2020

Regulation Text

Regulation Text

§170.315 (d)(3) *Audit report(s)—*

Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards in §170.210(e).

Standard(s) Referenced

Applies to entire criterion

§ 170.210(e)(1)

(i) The audit log must record the information specified in sections 7.1.1 through 7.1.3 and 7.1.6 through 7.1.9 of the standard specified in § 170.210(h) and changes to user privileges when health IT is in use.

(ii) The date and time must be recorded in accordance with the standard specified at § 170.210(g).

(2)

(i) The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at § 170.210(h) when the audit log status is changed.

(ii) The date and time each action occurs in accordance with the standard specified at § 170.210(g).

(3) The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at § 170.210(h) when the encryption status of electronic health information locally stored by EHR technology on end-user devices is changed. The date and time each action occurs in accordance with the standard specified at § 170.210(g).

§ 170.210(g) *Synchronized clocks*. The date and time recorded utilize a system clock that has been synchronized following (RFC 1305) Network Time Protocol or (RFC 5905) Network Time Protocol Version 4

§ 170.210(h) *Audit log content*. ASTM E2147-18 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems

Certification Companion Guide: Audit report(s) (Cures)

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* Final Rule (ONC Cures Act Final Rule). It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the ONC Cures Act Final Rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
Revised	No	Not Included	No

Certification Requirements

Design and Performance: Quality management system (§ 170.315(g)(4)) and accessibility-centered design (§ 170.315(g)(5)) must be certified as part of the overall scope of the certificate issued to the product.

- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, when different QMS are used, each QMS needs to be separately identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified

for every capability to which they were applied; or, alternatively the developer must state that no accessibility-centered design was used.

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))

Technical Explanations and Clarifications

Applies to entire criterion

Technical outcome –

- A user can create one or more audit reports for a specific time period that includes some or all of the data specified in sections 7.1.1, 7.1.2 and 7.1.6, through 7.1.9 of ASTM E1247-18; including changes to user privileges when health IT is in use; and record the date and time of the action in accordance with RFC 5905.
- The content included in each audit log is sortable.

Clarifications:

- The ONC Cures Act Final Rule included the requirement for Health IT Modules to support 7.1.3 Duration of Access in the ASTM E2147-18 standard. However, we have determined this requirement will not be in scope for testing and certifying to 2015 Edition Cures Update certification.
- The ONC Cures Act Final Rule included the requirement for Health IT Modules to support updates to audit logging and has incorporated by reference the standards, as amended effective June 30, 2020, § 170.299(1) ASTM E2147-18 Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, approved May 1 2018, IBR approved for §170.210(h).
- The ONC Cures Act Final Rule included the requirement for Health IT Modules to support the auditing requirements as specified in ASTM E2148-18. For the purposes of certification, sections 7.2 and 7.4 have been updated to sections 7.1.1 and 7.1.7. It is the expectation that the updated specification will be used.

- For purposes of certification, a Health IT Module should adhere to (RFC 5905) Network Time Protocol Version 4 for the synchronized clock requirement. The previous (RFC 1305) Network Time Protocol is obsolete and has been replaced by the updated standard.

For the purposes of certification, a Health IT Module may produce a single audit report with all of the specified auditable data or it may produce multiple audit reports with some portion of the required auditable data. However, if this latter approach is used, when all of the audit reports are considered together the total content they include must represent all of the required auditable data (which would be equivalent to the single audit report approach).

- If third party software is relied upon to meet the criteria, one of the following approaches applies:
  - Approach 1 requires disclosure of the software that was relied upon to meet the criterion.
  - Approach 2 requires documentation of how the external services that are necessary to meet the requirements of criteria will be deployed and used.
- A user could be a health care professional or office staff; or a software program or service that would interact directly with the certified health IT. [see 80 FR 62611; 77 FR 54168] A "user" is not a patient for the purposes of this criterion. [see also 77 FR 54168]
- For Health Information Service Provider (HISP) software that does not normally store patient data, certification to § 170.315 (d)(3) does not create the obligation to do so. Rather, certification to § 170.315 (d)(3) requires that a user is able to produce a forensic reconstruction of events in the case of a security incident. Audit reports would need to be generated that can sort and filter on the types of data identified in § 170.315 (d)(2).

Content last reviewed on June 22, 2020